SSH Sentinel

Quick Start Guide

MultiTech Systems

Quick Start Guide
82013152 Revision C
SSH Sentinel

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 2002, by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Record of Revisions

Revision	Date	Description
A	09/07/01	Manual released for SSH Sentinel v1.2.0.15.
B	04/30/02	Manual revised for SSH Sentinel v1.3, added license agreement, removed the RouteFinder portion of Setup example 3 (it exists in the RouteFinder Quick Start Guide).
C	10/15/02	Manual revised for SSH Sentinel V.1.4.

Patents

This product is covered by one or more of the following U.S. Patent Numbers: **5.301.274; 5.309.562**; **5.355.365; 5.355.653; 5.452.289; 5.453.986**. Other Patents Pending.

Trademarks

Trademarks of Multi-Tech Systems, Inc.: Multi-Tech, the Multi-Tech logo, and RouteFinder.
Windows is a registered trademark of Microsoft Corporation in the United States and other countries. SSH, ssh, SSH Secure Shell, and SSH Sentinel are trademarks or registered trademarks of SSH Communications Security Corp.
All products or technologies are the trademarks or registered trademarks of their respective holders.

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Tech Support (800) 972-2439
Internet Address: http://www.multitech.com

Contents

Chapter 1 – Introduction and Description 1

Internet Protocol (IP) 2
Internet Protocol Security (IPSec) 2
About This Manual and Related Manuals 3
Ship Kit Contents 3

Chapter 2 – SSH Sentinel Client Installation and Setup 4

Introduction 4
Pre-Installation Requirements 4
Starting the SSH Sentinel Installation 5
Authentication Key Generation 10
Certificate Information 12
Choose the Enrollment Method 13
Encryption Speed Diagnostics 16
Completing the Installation 17

Chapter 3 – Client Setup Examples 18

LAN to SSH Sentinel Client 18
Sentinel Configuration 21

Chapter 4 – Updating and Removing SSH Sentinel 32

Updating SSH Sentinel 32
Removing SSH Sentinel 32

Appendix A – Technical Support 33

Contacting Technical Support 33
Recording RouteFinder Information 33

Appendix B – SSH Sentinel CD 34

Appendix C – Multi-User Software License Agreement 35

Chapter 1 – Introduction and Description

Welcome to world of Internet security. SSH Sentinel is a software product that secures network communications on a Windows workstation. Network traffic (IP traffic – Internet Protocol) is protected using the IPSec (Internet Protocol Security) protocol as specified by the Internet Engineering Task Force (IETF) standards.

SSH Sentinel is an easy-to-use product designed for end users. It allows you to encrypt and authenticate important network connections, like remote access to corporate networks remote administration, file transfer, sending and receiving email (SMTP, POP) and IP telephony.

SSH Sentinel is a companion software package for Multi-Tech's RouteFinders RF650VPN and RF550VPN.

The RF650VPN is an Internet security appliance that lets you use data encryption and the Internet to securely connect to telecommuters, remote offices, customers, or suppliers while avoiding the cost of expensive private leased lines.

The RF550VPN is an Internet security appliance designed for the small branch office or telecommuter who needs secure access to the corporate LAN.

The SSH Sentinel IPSec VPN Client software is available in 1-, 5-, 10- and 50-user packages. The RF650VPN provides SSH Sentinel version 1.4 client software (30-day trial version with Static IP support). It allows client computer connection to the RouteFinders using PSK (Pre Shared Keys) in a Host-to-Net connection.

Chapter 2 of this manual describes the SSH Sentinel client installation and setup process for the 1-, 5-, 10- or 50-user Sentinel packages with these Multi-Tech product package numbers:

Product Packages	**Description**
RFIPSC-1	SSH Sentinel 1-User License
RFIPSC-5	SSH Sentinel 5-User License
RFIPSC-10	SSH Sentinel 10-User License
RFIPSC-50	SSH Sentinel 50-User License

SSH Sentinel software currently supports the following Microsoft Windows operating systems: Windows 95, Windows 98, Windows NT4, Windows Me, Windows 2000, and Windows XP.

SSH Sentinel is designed to be a *client* type IPSec application. The features are designed for a single user workstation using a single network adapter and the Internet Protocol (IP). SSH Sentinel supports all network connection types, including dial-up. The product is designed to be secure and robust, easy to use and quick to adapt to the environment at hand.

Key characteristics include intuitive installation and configuration, as well as an easy way to use certificates for authentication.

Internet Protocol (IP)

The open architecture of the Internet Protocol (IP) makes it a highly efficient, cost-effective, and flexible communications protocol for local and global communications.

IP is widely adopted, not only on the global Internet, but also in the internal networks of large corporations.

The Internet Protocol was designed to be highly reliable against random network errors. However, it was not designed to be secure against a malicious attacker. In fact, it is vulnerable to a number of well-known attacks. This is preventing it from being used to its fullest for business and other purposes involving confidential or mission-critical data. The most common types of attacks include:

- Eavesdropping on a transmission, for example, looking for passwords, credit card numbers, or business secrets.
- Taking over communications, or hijacking communications, in such a way that the attacker can inspect and modify any data being transmitted between the communicating parties.
- Faking network addresses, also known as IP spoofing, in order to fool access control mechanisms based on network addresses, or to redirect connections to a fake server.

To prevent this misuse and attacks on IP, the Internet Engineering Task Force (IETF) has developed the Internet Protocol Security (IPSec) protocol suite.

Internet Protocol Security (IPSec)

The Internet Engineering Task Force (IETF) has developed the Internet Protocol Security (IPSec) protocol suite to prevent misuse and attacks on IP. IETF is an international standards body with representation from hundreds of leading companies, universities, and individuals developing Internet-related technologies. Its track record includes the Internet Protocol itself and most of the other protocols and technologies that form the backbone of the Internet.

The IPSec protocol suite adds security to the basic IP version 4 protocol and is supported by all leading vendors of Internet products. IPSec is a mandatory part of the next generation of IP protocol, IP version 6. The IPSec protocol works on the network level. It adds authentication and encryption to each data packet transmitted. It protects each packet against eavesdropping and modification and provides authentication of the origin of the packet.

IPSec works independently of any application protocol. Thus, all applications that use IP protocol for data transfer are equally and transparently protected. IPSec makes it safe to use the Internet for transmitting confidential data. By doing so, it solves the main obstacle that is slowing down the adoption of the Internet for business use.

About This Manual and Related Manuals

This Quick Start Guide is intended to provide the experienced client user or system administrator with the information needed to quickly get the SSH Sentinel software up and running.

The full SSH Sentinel User Guide is provided on the SSH Sentinel CD-ROM included in the package.

Please address comments about this manual to the Multi-Tech Publications Dept.

Related manuals may include add-on product documentation for options such as the Windows PPTP client, the E-mail Anti-Virus Upgrade, etc.

This document may contain links to sites on the Internet, which are owned and operated by third parties. Multi-Tech Systems, Inc. is not responsible for the content of any such third-party site.

Ship Kit Contents

The SSH IPSec Client License Pak is shipped with the following:

- one SSH IPSec Client CD-ROM
- one SSH IPSec Client License
- one printed Quick Start Guide manual
- one Multi-User Software License Agreement
- one Registration Card

If any of these items are missing, contact Multi-Tech Systems or your dealer or distributor. Inspect the contents for signs of any shipping damage. If damage is observed, do not install the software; contact Multi-Tech's Tech Support for advice.

Chapter 2 – SSH Sentinel Client Installation and Setup

Introduction

This section describes the SSH Sentinel software, an IPSec client product by SSH Communications Security Corp, providing secure communications over a TCP/IP connection. The Sentinel SSH software is used by client devices for secure connection to Multi-Tech's RouteFinders RF650VPN and RF550VPN. The SSH Sentinel client installation and setup procedures are described in the following sections.

The installation of the SSH Sentinel software is a straightforward process guided by an installation wizard, and you should be able to complete it without studying this manual. The beginning of this section describes the first installation of the SSH Sentinel software. During the installation, you create an authentication key pair and a matching certificate to be used for authentication. However, if a previous version of the software is already installed on your computer, then launching the installation only updates the existing software to the new version. The security policy rules and the authentication keys that you have configured with the previous version of the software are preserved. You can always remove the software completely and then reinstall it.

Pre-Installation Requirements

SSH Sentinel client software works on the following Microsoft Windows platforms and versions:

Platform	Version Build	Notes
Windows 95	OSR1, OSR2	Winsock2 required
Windows 98	SE	-
Windows NT 4.0	SP3 to SP6	-
Windows Me		-
Windows 2000	SP1	-
Windows XP		

SSH Sentinel is a client-type implementation of IPSec; it is not IPSec gateway software, even though some of the Windows platforms are capable of functioning as routers. Before starting SSH Sentinel client installation, make sure that there are no other IPSec implementations, network sniffers, NAT applications, firewalls, or third party intermediate network drivers installed. SSH Sentinel may affect the functionality of such software.

The SSH Sentinel installation requires that you have full access rights for the system files on your computer. On a Windows NT system, you must log in with administrator rights.

To run the SSH Sentinel client software, you need a personal computer with at least the following configuration:

- Processor: Pentium 100 MHz
- Memory (RAM): 32 MB for Windows 9x, or 64 MB for Windows NT4/2000
- Hard disk space: 10 megabytes of free disk space
- Network connection: TCP/IP network protocol
- A CD-ROM drive

Starting the SSH Sentinel Installation

The SSH Sentinel installation requires that you have full access rights for the system files on your computer. On a Windows NT system, you must log in with administrator rights.

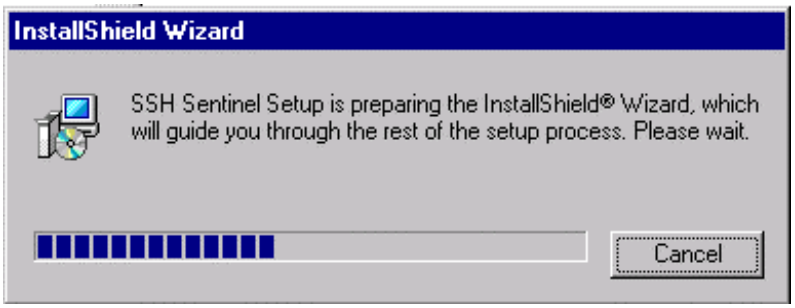
1. Insert the Client CD into the CD-ROM drive. The startup screen displays in your Web browser.

SSH Sentinel IPsec Client
Install IPsec Client Software.
Read the End User Licensing Agreement.
Read the Installation User Guide.
Read the Installation Quick Start Guide.
Register your product at www.multitech.com.

2. Click **Install IPSec Client Software.**
   The **File Download** screen displays.
   - Select **Run this program from its current location**
   - Click **OK**.

3. The **Do you want to install and run** screen displays.
   - Click **Yes**.

4. The SSH Sentinel Setup InstallShield® Wizard screen displays.


InstallShield Wizard
SSH Sentinel Setup is preparing the InstallShield® Wizard, which will guide you through the rest of the setup process. Please wait.
Cancel

The self-extracting package automatically initiates InstallShield® software to install and set up SSH Sentinel Client software. On the Installation screen, click **Next**.

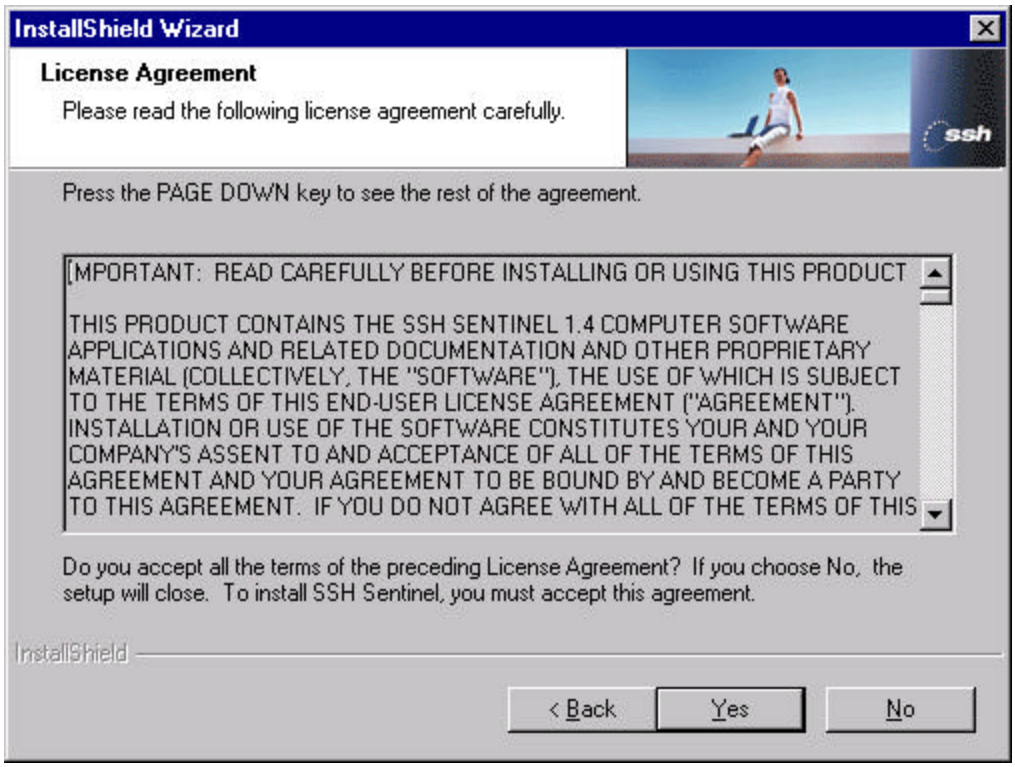
InstallShield Wizard
ssh
Welcome to the InstallShield Wizard for SSH Sentinel
The setup is about to install SSH Sentinel security software on your computer. To continue, click Next.
SSH Sentinel (TM) Version 1.4
Copyright © 2000 - 2002 SSH Communications Security Corp. This software is protected by international copyright laws. All rights reserved.
ssh® is a registered trademark of SSH Communications Security Corp in the United States and in certain other jurisdictions. The SSH logo, SSH Sentinel and Making the Internet Secure are trademarks of SSH Communications Security Corp and may be registered in certain jurisdictions. All other names and marks are property of their respective owners.
< Back
Next >
Cancel

The installer will run the Installation Wizard, which creates the initial configuration and sets up the SSH Sentinel client software.

Note: If a previous version of the SSH Sentinel software is installed on your computer and you try to install a new version, the wizard updates the software and the steps described here are skipped.

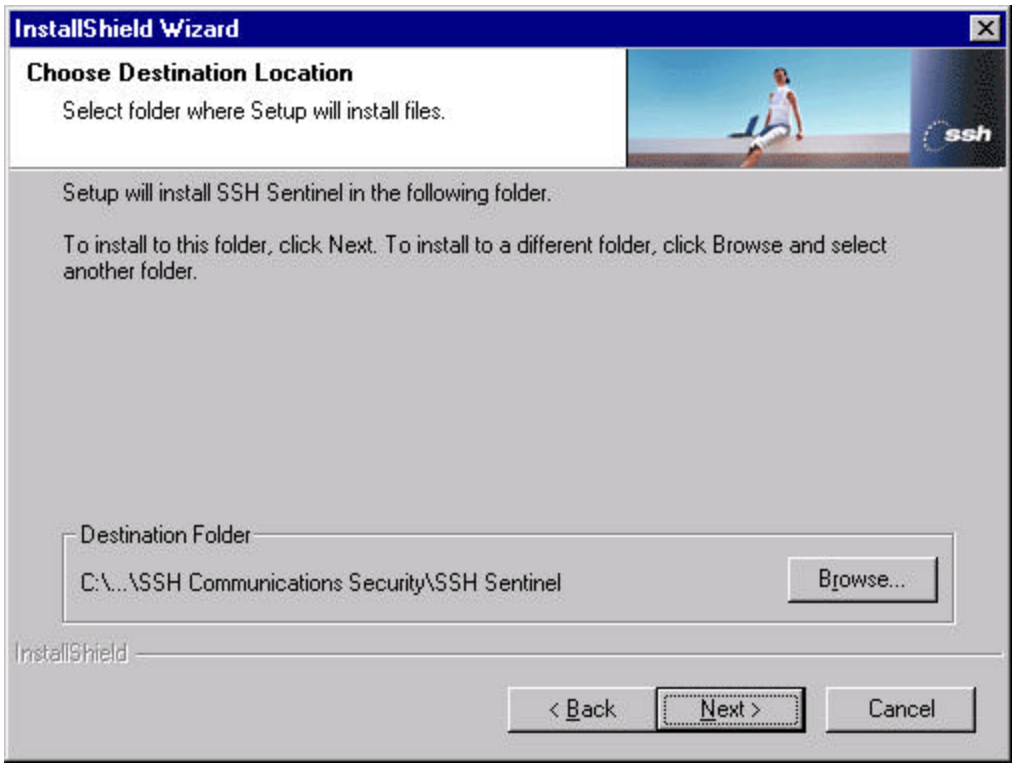
5. When started, the Installation Wizard goes through a sequence of basic installation dialogs, displaying the licensing agreement and allowing you to select the installation directory and the program folder. The installation can only be performed on a local computer. Remote installation of SSH Sentinel is not possible, because the installation program updates kernel mode components related to networking and remote access.

   Click **Yes** to accept the terms of the agreement.

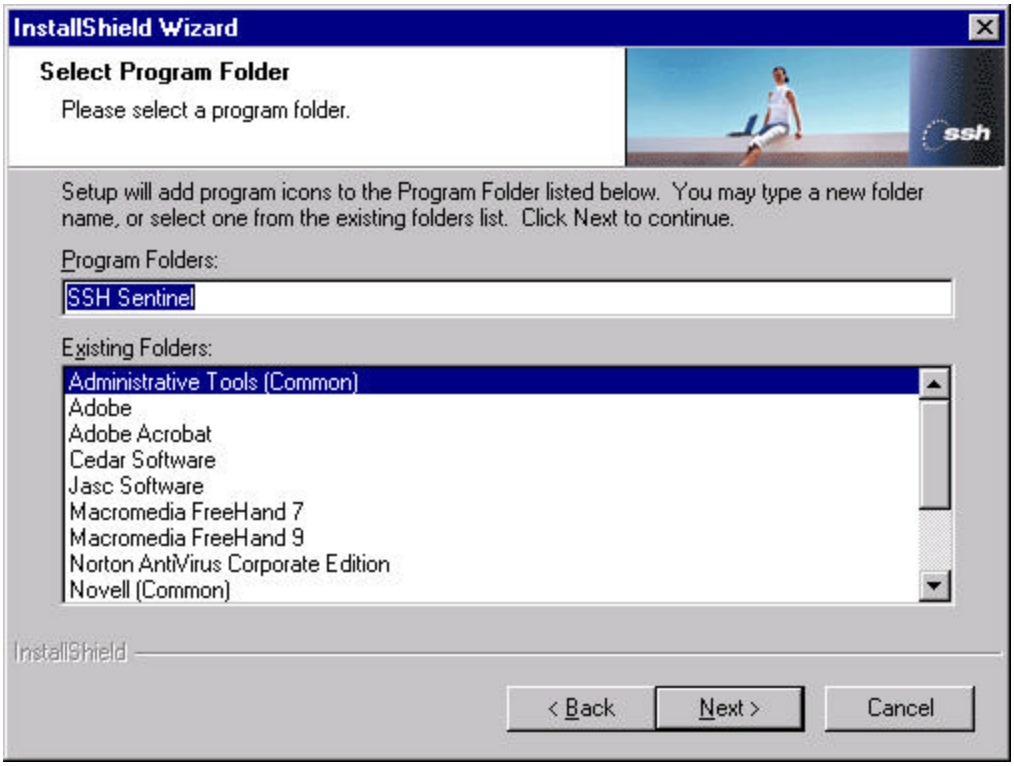

InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
ssh
Press the PAGE DOWN key to see the rest of the agreement.
IMPORTANT: READ CAREFULLY BEFORE INSTALLING OR USING THIS PRODUCT
THIS PRODUCT CONTAINS THE SSH SENTINEL 1.4 COMPUTER SOFTWARE APPLICATIONS AND RELATED DOCUMENTATION AND OTHER PROPRIETARY MATERIAL (COLLECTIVELY, THE "SOFTWARE"), THE USE OF WHICH IS SUBJECT TO THE TERMS OF THIS END-USER LICENSE AGREEMENT ("AGREEMENT"). INSTALLATION OR USE OF THE SOFTWARE CONSTITUTES YOUR AND YOUR COMPANY'S ASSENT TO AND ACCEPTANCE OF ALL OF THE TERMS OF THIS AGREEMENT AND YOUR AGREEMENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE WITH ALL OF THE TERMS OF THIS
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install SSH Sentinel, you must accept this agreement.
InstallShield
< Back
Yes
No

   Note that the installation will terminate immediately if you do not click **Yes** to accept the licensing agreement.

6. The **Choose Destination Path** displays.


InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
ssh
Setup will install SSH Sentinel in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\...\SSH Communications Security\SSH Sentinel
Browse...
InstallShield
< Back
Next >
Cancel

7. Choose your Destination Path and click **Next,** then select a destination folder for the SSH Sentinel icon and click **Next>.**



Next, the **Setup Status** screen displays to let you know that SSH Sentinel is performing the requested operations. Once the operations are complete, the **Authentication Key Generation** screen displays.

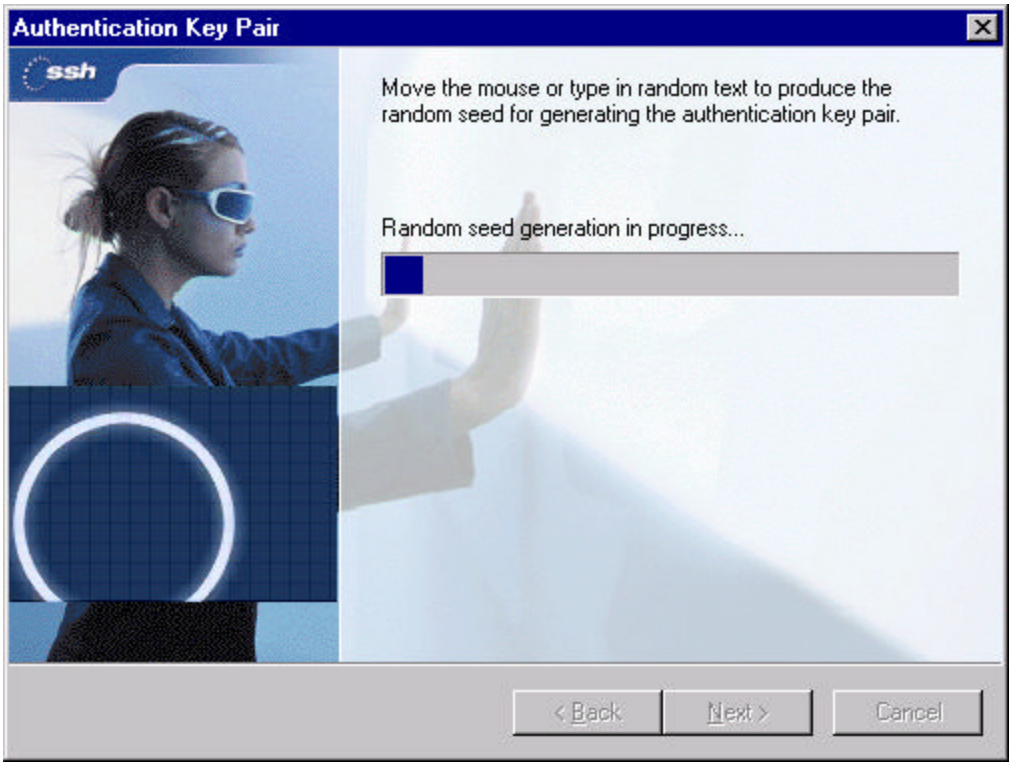
Authentication Key Generation

8. On this screen, move your mouse or type some random text to generate a host authentication keypair.

   When complete, click **Next**.

   The SSH Sentinel Installation Wizard generates a primary authentication key for IPSec peer (host) authentication purposes. The primary authentication key is a 1024-bit RSA key pair that is used for digital signatures and strong authentication.

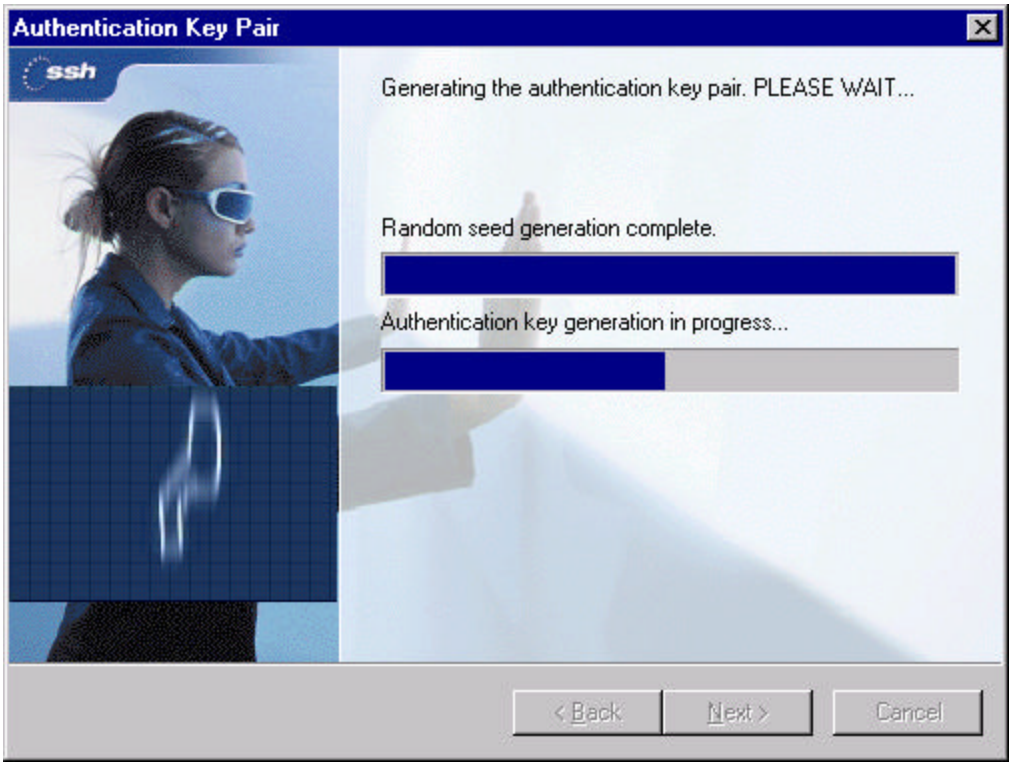
   Authentication key generation begins with random seed generation. A random pool of data is collected from the user moving the mouse or typing in random text. The data is then used as a seed to ensure that all authentication keys will be unique. With this method, the likelihood of generating two identical authentication keys is infinitesimal.


Authentication Key Pair
ssh
Move the mouse or type in random text to produce the random seed for generating the authentication key pair.
Random seed generation in progress...
< Back
Next >
Cancel

   The general level of security that can be provided with 1024-bit RSA authentication keys is considered military strength. The Internet Key Exchange (IKE) protocol used in key negotiation is better by design and security than most of the other solutions that currently exist.

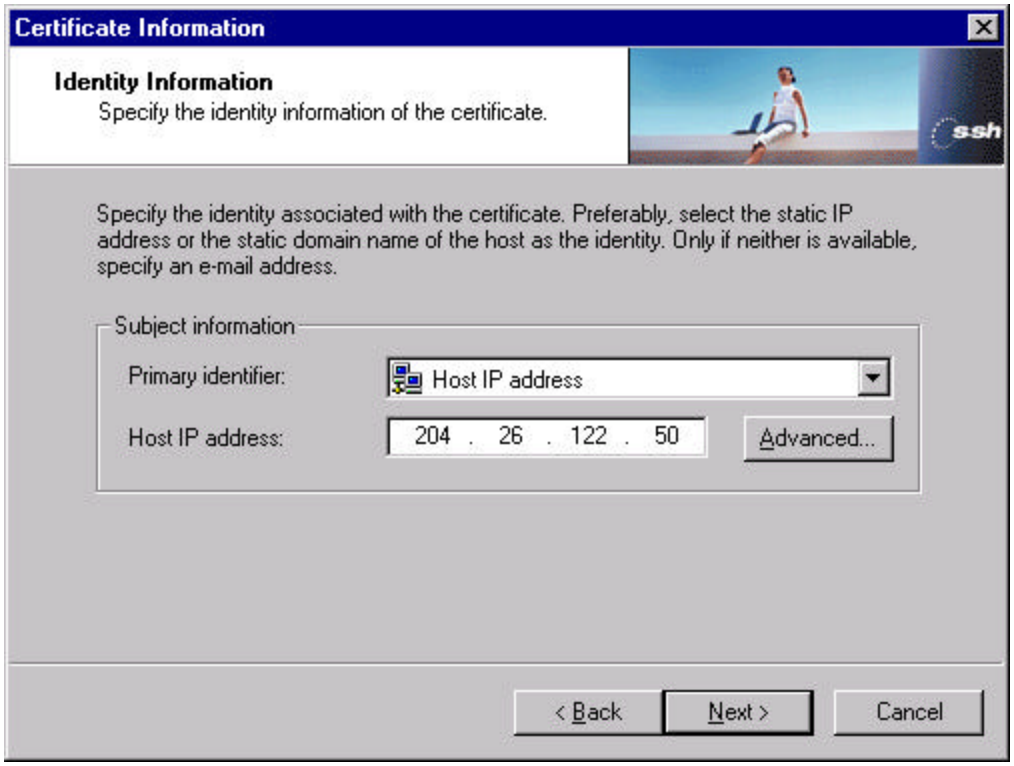
   The SSH Sentinel key generation process will take some 30 seconds and may momentarily use most of the computer's CPU resources.

9. Once the authentication key generation is complete, click **Next>** to proceed with the installation.



Certificate Information

10. Enter the information to identify the authentication key. SSH Sentinel uses certificates and digital signatures as its primary authentication method. SSH Sentinel processes certificates according to the IETF Public-Key Infrastructure X.509v3 standards, allowing you to take advantage of the public-key infrastructure (PKI). SSH Sentinel supports certificate revocation lists (CRLs) and authority revocation lists (ARLs, that is, CRLs for CAs) and is very configurable. However, you can run the software as stand-alone, separately from any public-key infrastructure.

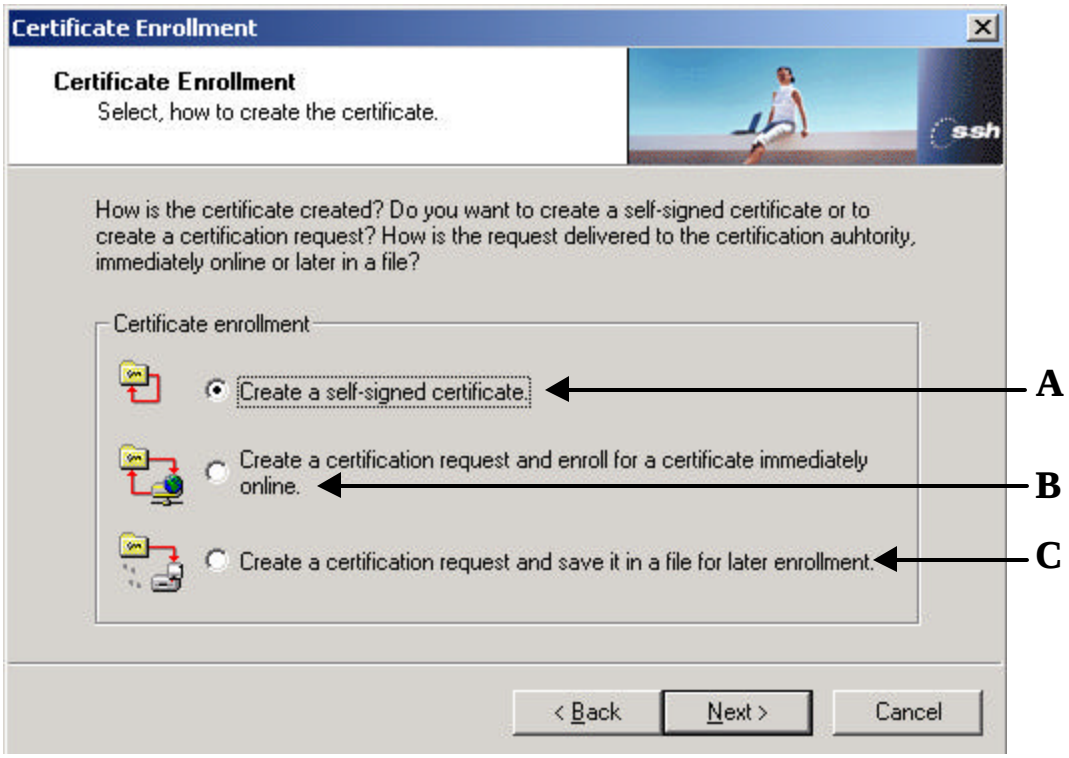

Certificate Information
Identity Information
Specify the identity information of the certificate.
ssh
Specify the identity associated with the certificate. Preferably, select the static IP address or the static domain name of the host as the identity. Only if neither is available, specify an e-mail address.
Subject information
Primary identifier:
Host IP address
Host IP address:
204 . 26 . 122 . 50
Advanced...
< Back
Next >
Cancel

The setup requires host identity information that is to be associated with the authentication key pair and its certificate. A commonly preferred identity is the host DNS name, also referred to as the Fully Qualified Domain Name (FQDN). The DNS name should be used as the identity whenever the host has a static DNS name and whenever it is safe to assume that name service will be available. If the host does not have a static DNS name, its static IP address may be used as the host identity.

If neither static DNS name nor IP address is available, you may use an email address as the identity. However, using an email address as the identity makes it difficult for remote hosts to bind IPSec rules for the host, since rules are normally bound to a host name or an IP address.

Choose the Enrollment Method

11. Choose your **Certificate Enrollment Protocol** and click **Next>**.
    A certification request can be created as part of the installation process. You can either enroll online, in other words create and send the request immediately, or save the request in a file and deliver it later to the certification authority (CA). If there is no certification authority available or you for some reason want to postpone the creation of the request, create a self-signed certificate. It should be noted that once you've installed the software, you can create as many certification requests as you wish with the SSH Sentinel user interface but you cannot create a self-signed certificate with it.


Certificate Enrollment
Certificate Enrollment
Select, how to create the certificate.
ssh
How is the certificate created? Do you want to create a self-signed certificate or to create a certification request? How is the request delivered to the certification auhtority, immediately online or later in a file?
Certificate enrollment
Create a self-signed certificate.
Create a certification request and enroll for a certificate immediately online.
Create a certification request and save it in a file for later enrollment.
A
B
C
< Back
Next >
Cancel

Your choices for **Certificate Enrollment Protocol** are:

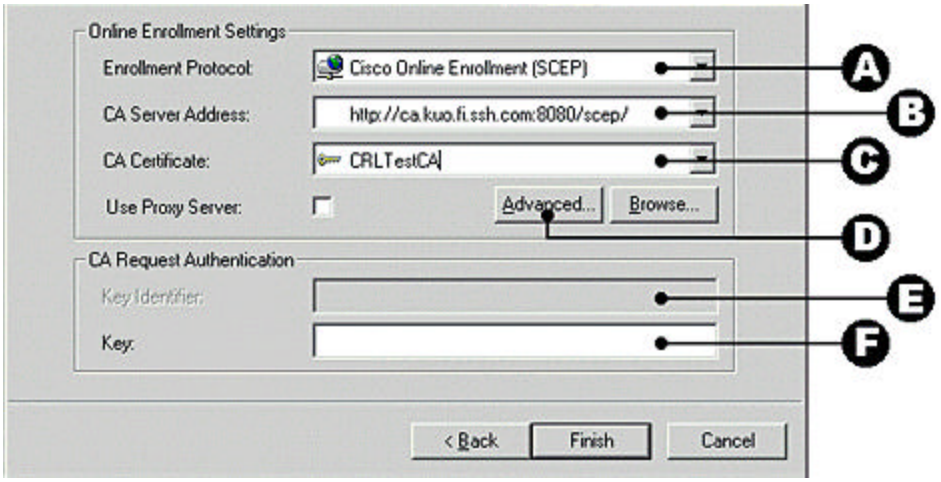
A - To create a **self-signed** certificate, select option **A** as indicated above. The keys created in the previous step are used when the system creates the certificate.

B - To issue an online certification request, select the option **B** as indicated above. The installation wizard displays a dialog box in which further information about the certification authority and the enrollment protocol can be entered.

C - To create a certification request for later processing, select option **C** as indicated above.

SSH Sentinel Online Enrollment Information

To enroll online, you must locate the certification authority server and you must possess the certification authority certificate. Most often, you can download the certificate of the certification authority from its web site.



You must specify the enrollment protocol. In addition, you may configure the Socks and proxy settings to get through the firewall if the local server is protected by one.

Enrollment Protocol (A)
Select the enrollment protocol from the drop-down list. Naturally, you should choose a protocol that is supported by the certification authority. The following protocols are available: Simple Certificate Enrollment Protocol (SCEP) and Certificate Management Protocol (CMP).

CA Server Address (B)
Specify the address (URL) of the certification authority web site.

CA Certificate (C)
The certificate of the certification authority is needed to encrypt the certification request before sending it to the certification authority. You can usually fetch it from the authority's Web site.

In the drop-down menu, you see the possibilities on how to import the certification authority certificate into the request: The most convenient way is to specify here the URL where the certificate is located. In this case, the certificate must be in PEM encoded format. SSH Sentinel then automatically fetches the certificate from the web site. You may also have downloaded the certificate earlier using a web browser and either saved it in a file or copied the contents of it to the Windows clipboard. In a file, the certificate may be in binary (X.509), PEM (Privacy Enhanced Mail) or HEX format. Pasted from the clipboard, the certificate must be in PEM encoded format.

Advanced button (D)
Opens a dialog box for configuring the socks and proxy settings.

Reference Number (E) (Key Identifier)
The key identifier is used ***only in connection with the Certificate Management Protocol (CMP).*** The key identifier is used along with the key to identify the user requesting a certificate.

Key (F)

This selection is used ***only in connection with the CMP protocol***. The **Key** selected is a shared secret granted by the certification authority to be used in the certification request. This **Key** is used for verification of the user requesting a certificate.

Off-line Certification Request

An off-line certification request is simply a file, where the request is stored for later use. The request is of PKCS#10 format and saved in Privacy Enhanced Mail (PEM) encoded format.

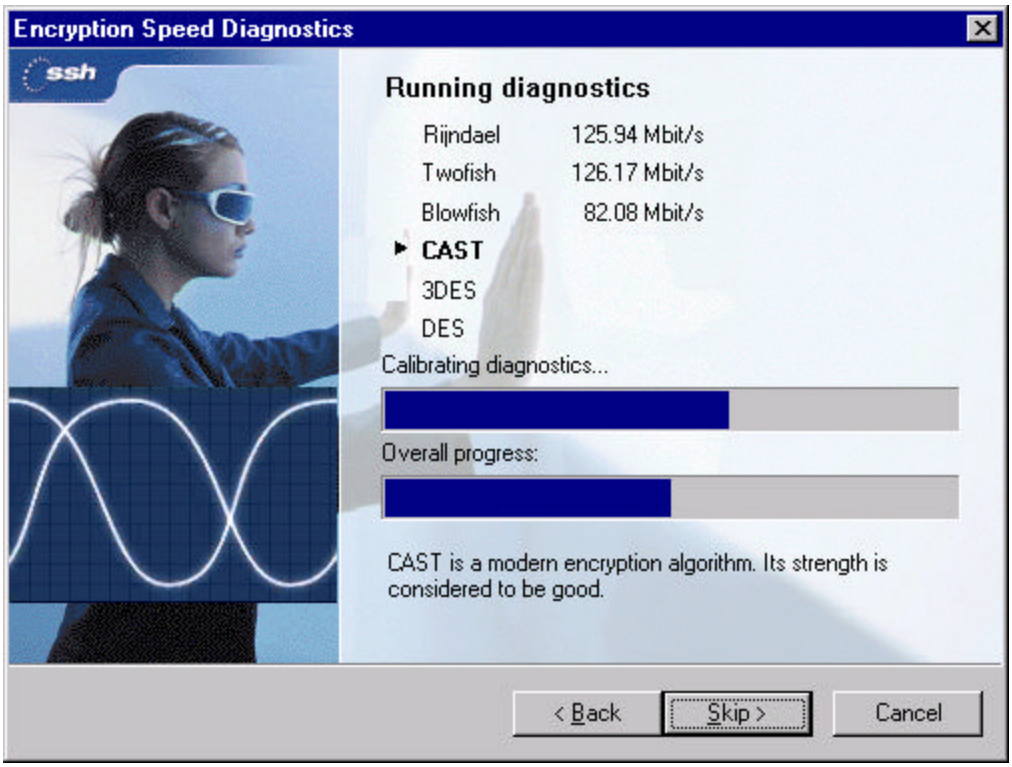
To complete the enrollment, you must deliver the request to the certification authority.
You might save the request on a floppy disk and deliver the floppy to the authority, or you may prefer sending the request via email or using an enrollment service on the Web.

Select PKCS#10 request file location

In the text field (callout A in Figure 10 above), enter the path and the name of the file where the certification request will be stored. You can also click the **Browse** button to select. Click **Next** and continue installation.

Encryption Speed Diagnostics

12. Let the algorithm diagnostics run or skip them. SSH Sentinel runs diagnostics on the encryption algorithms as the last step of the installation. You can bypass this step by clicking the **Skip>** button on the dialog box. These diagnostics reveal the speeds of the encryption algorithms compared to each other. SSH Sentinel supports the following ciphers: Rijndael, Twofish, Blowfish, Cast, 3DES and DES.



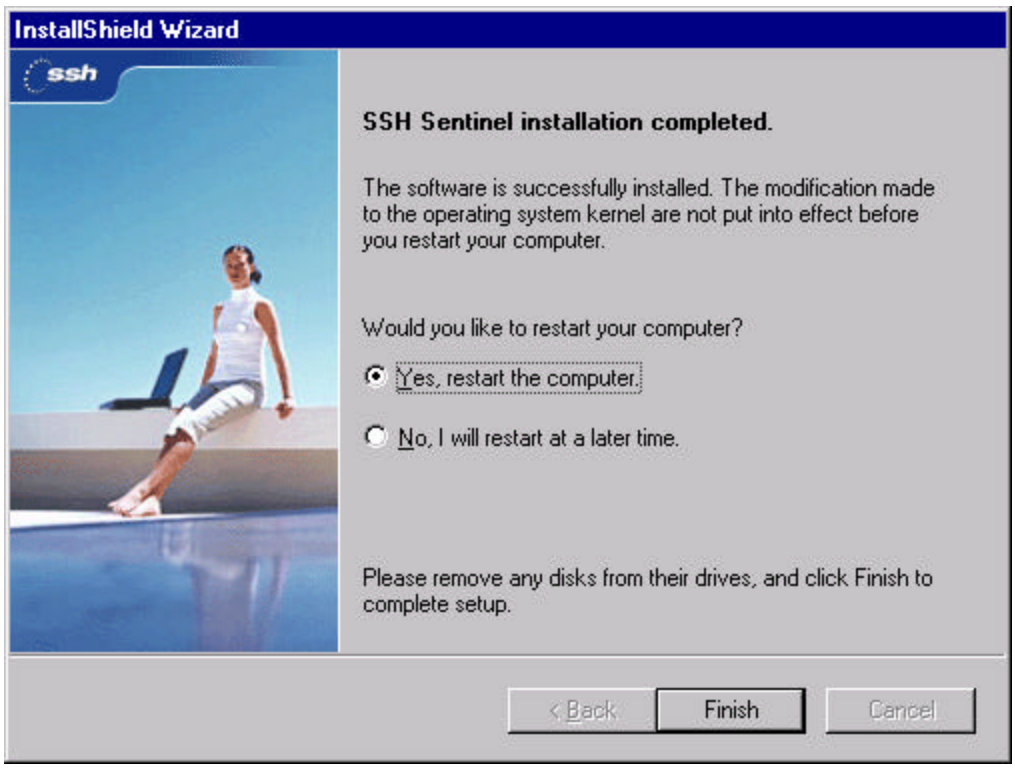
With the exception of DES, all of these ciphers can be considered secure for commercial use. The DES encryption algorithm is supported as a fallback option for interoperability reasons. Rijndael, an encryption algorithm widely considered fast, secure and reliable, is used as the default cipher by SSH Sentinel.

The diagnostics also reveal the relative speed of your computer running the algorithms. There is a lot of contradictory information available on encryption speeds. The diagnostics give you the chance to use your own judgment. The diagnostics measure the encryption speed of your computer within the memory. The data packets are not transmitted to the network. This is a common way to measure performance by encryption hardware vendors. It has the advantage of giving simple figures on the speed: Due to a number of variables that affect the final result, it would be very complicated to define a standard environment in which to reliably measure the overall network throughput. Moreover, the real-world network throughput simply cannot be measured during the installation, because the kernel-mode IPSec engine is not available before the first reboot.

An Intel P3 personal computer with processor speed of 800 MHz should be able to provide a maximum IPSec throughput of over 40 Mbit/s on the preferred cipher. However, other variables, such as the operating system, network bandwidth and CPU load, naturally set limitations to the throughput.

Completing the Installation

13. Click **Finish** and re-start your computer (recommended). The installation of the SSH Sentinel client software adds kernel-mode components to the operating system network management. For this reason, you must restart the computer before using the SSH software.


InstallShield Wizard
ssh
SSH Sentinel installation completed.
The software is successfully installed. The modification made to the operating system kernel are not put into effect before you restart your computer.
Would you like to restart your computer?
Yes, restart the computer.
No, I will restart at a later time.
Please remove any disks from their drives, and click Finish to complete setup.
< Back
Finish
Cancel

The SSH Sentinel installation is complete. Proceed to the next section for SSH IPSec client setup.

Chapter 3 – Client Setup Examples

LAN to SSH Sentinel Client

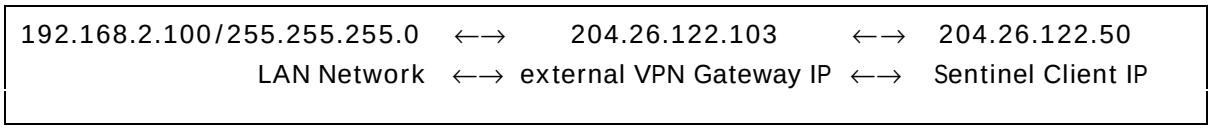
(Static IP) to connect to a RouteFinder using Pre Shared Keys (PSK)

This section describes how to set up a Host to Net connection between an SSH Sentinel client and a RouteFinder.

Before you can setup the SSH Sentinel client, you will have to configure your gateway. For gateway configuration, see Multi-Tech's RouteFinder RF650VPN documentation, Multi-Tech's RouteFinder RF550VPN documentation, or other vendor's documentation.

This Quick Start Guide covers only the SSH Sentinel client setup.

The following diagrams show a LAN network configured to communicate through an external VPN gateway to an SSH Sentinel client.



LAN-to-Client Setup Using:

- Multi-Tech's RouteFinder RF550VPN to connect the LAN at Site A to the external VPN gateway.
- SSH Sentinel to connect a remote client to the VPN gateway to the LAN at Site A.

The information to the left of the diagram is a list of Multi-Tech's RF550VPN configuration for this example.

SSH Sentinel Client accessing LAN Through RF550VPN RouteFinder

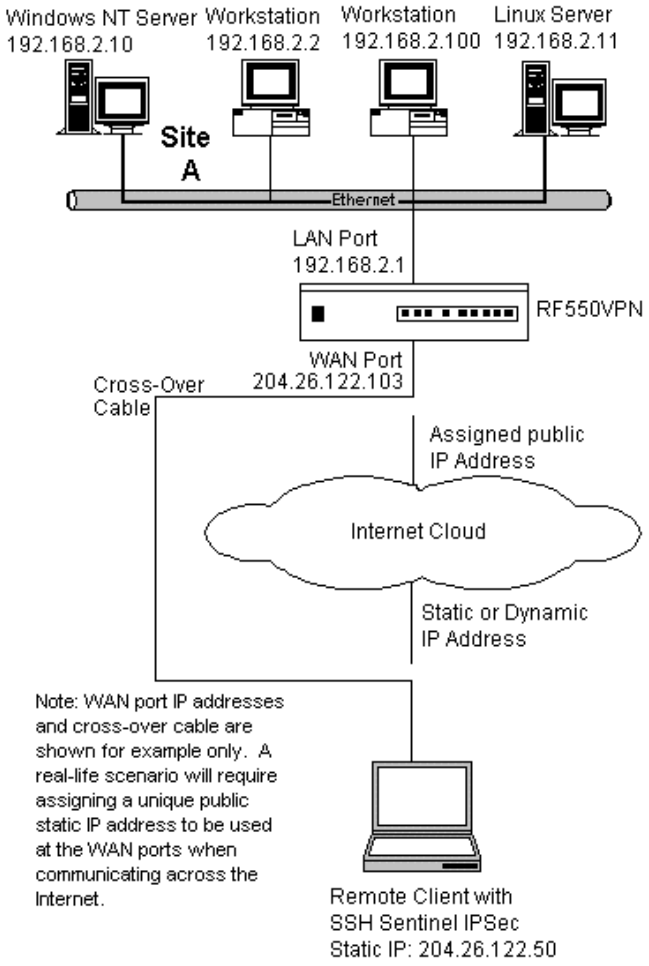
1. Domain name = StaticSentinel

2. Public Class C = 204.26.122.x

3. SETUP WIZARD | DEVICE IP SETTINGS
   IP Address: 192.168.2.1
   IP Subnet Mask: 255.255.255.0

4. SETUP WIZARD | CABLE/xDSL ISP SETTINGS
   Check 'Your ISP requires you to input IP settings'
   IP assigned by your ISP: 204.26.122.103
   IP Subnet Mask: 255.255.255.0
   ISP Gateway Address: 204.26.122.50
   Domain Name Server: 0.0.0.0

5. SETUP WIZARD | VPN SETTINGS
   Connection Name = IPSec Pass Through
   Disable UID
   Remote IP Network = 204.26.122.50 (static IP)
   Remote IP Network = 0.0.0.0 (dynamic IP)
   Remote IP Netmask = 255.255.255.255 (static IP)
   Remote IP Netmask = 0.0.0.0 (dynamic IP)
   Remote Gateway IP = 204.26.122.50 (static IP)
   Remote Gateway IP = 0.0.0.0 (dynamic IP)
   Network Interface = WAN Ethernet
   Secure Association = Enable IKE
   Perfect Forward Secure = Enable
   Encryption Protocol = 3DES
   Preshared Key = 1o2t3t4f
   Key Life = Set to default
   IKE Life Time = Set to default



LAN-to-Client Setup Using:

- Multi-Tech's RouteFinder RF650VPN to connect the LAN at Site A to the external VPN gateway.
- SSH Sentinel to connect a remote client to the VPN gateway to the LAN at Site A.

The information to the left of the diagram is a list of Multi-Tech's RF650VPN configuration for this example.

Remote Client-to-LAN Configuration Using SSH Sentinel with Static IP

1. Domain name = site-A.com

2. Public Class C = 204.26.122.x

3. Definitions | Network
   LAN - 192.168.2.0 - 255.255.255.0
   Sentinel Client - 204.26.122.50 - 255.255.255.255

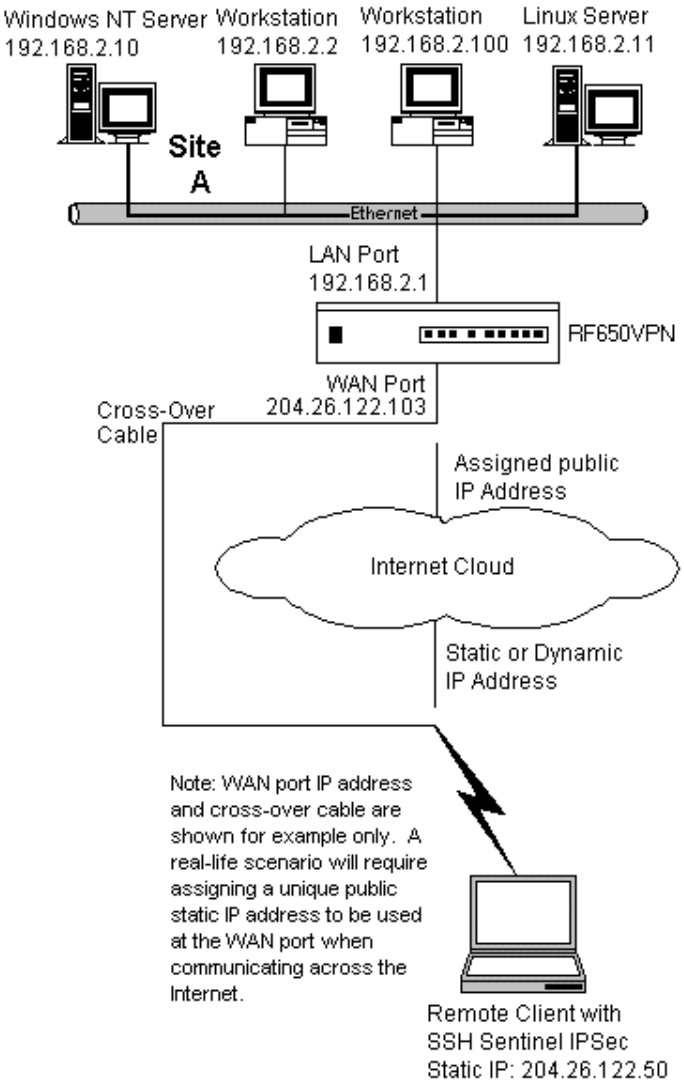
4. Network | Interfaces
   Default gateway = 204.26.122.1
   Host name = fw.site-A.com
   eth0 = LAN, 192.168.2.1, 255.255.255.0
   eth1 = WAN, 204.26.122.103, 255.255.255.0
   eth2 = DMZ(don't care)

5. Network | Masquerading
   LAN --> WAN

6a. Packet Filter | Rules (Remote client static IP)
   LAN - Any - Any- Allow
   Sentinel Client - Any - Any - Allow

6b. Packet Filter | Rules (Remote client dynamic IP)
   Any - Any - Any - Allow

7. VPN | IPSec Configurations
   Enable IPSec Status
   Enable IKE-debugging (optional)
   * name = Sentinel
   * Perfect Secret Forwarding = yes
   * Secure Association = ike
   * Authentication method = secret
   * Enter secret key
   * Local Interface = WAN
   * Local subnet = LAN
   * Remote IP = Any (remote client dynamic IP)
   * Remote IP = Sentinel Client (remote client static IP)
   * Remote subnet = (blank)

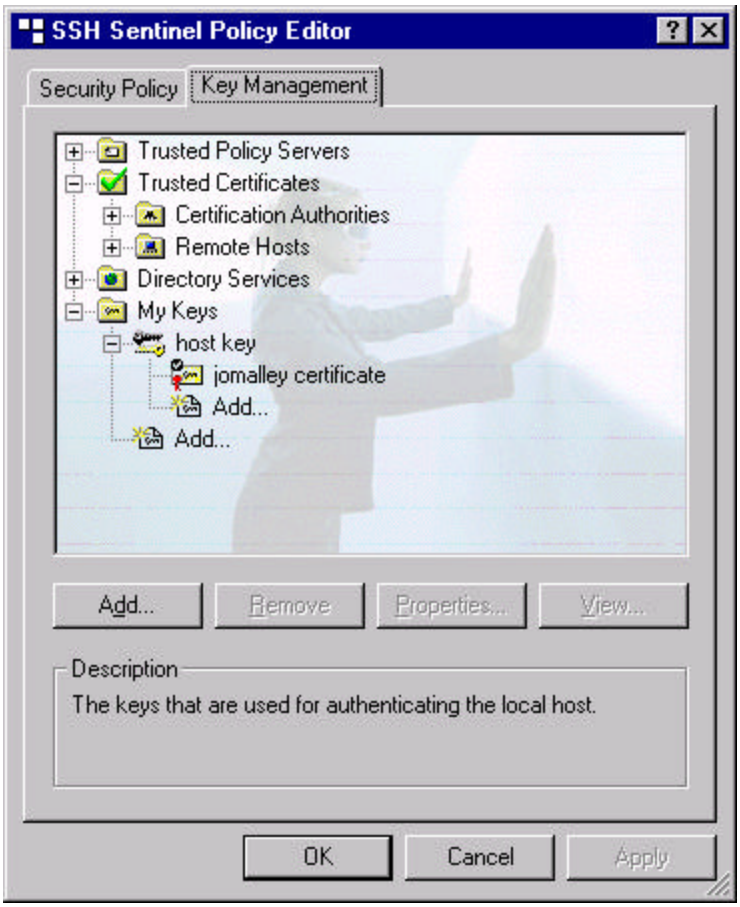


Sentinel Configuration

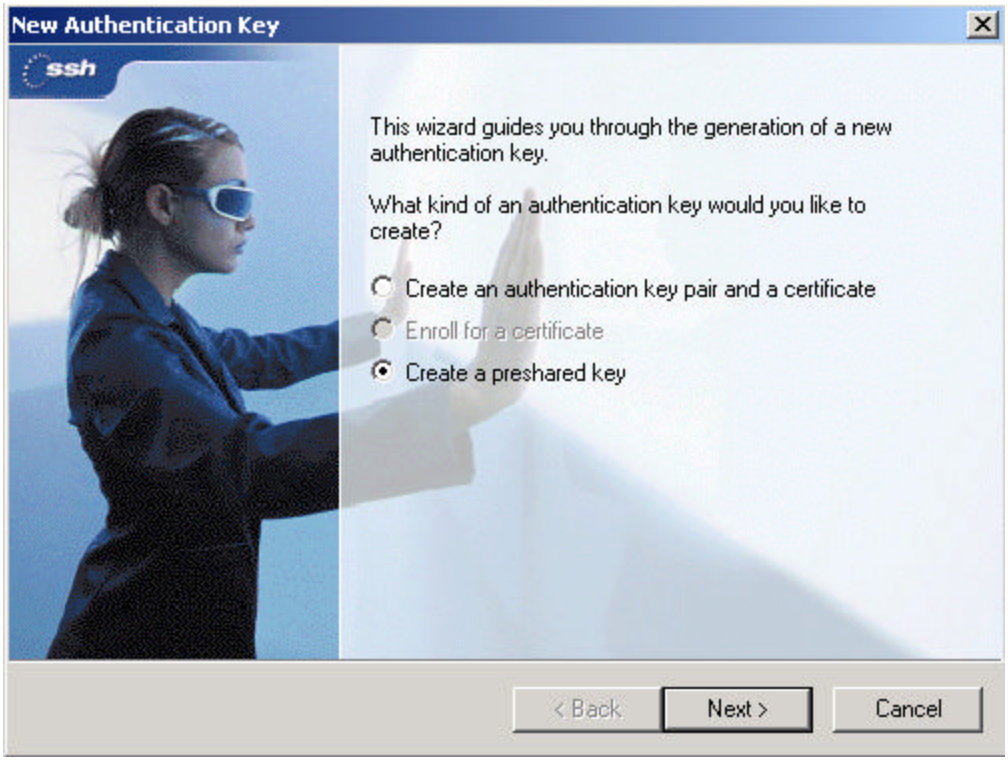
1. Select the **Sentinel Policy Editor** ( ) icon located on your task bar.

   Then click Run Policy Editor...

2. Click the **Key Management** tab at the top of the SSH Sentinel Policy Editor window.
3. Highlight **My Keys** and click the **Add** button to create a new Authentication Key.



4. The **New Authentication Key** screen displays. Click the **Create a Preshared Key** button. Click **Next.**


New Authentication Key
ssh
This wizard guides you through the generation of a new authentication key.
What kind of an authentication key would you like to create?
Create an authentication key pair and a certificate
Enroll for a certificate
Create a preshared key
< Back
Next >
Cancel

5. The **Create a Preshared Key** screen displays.

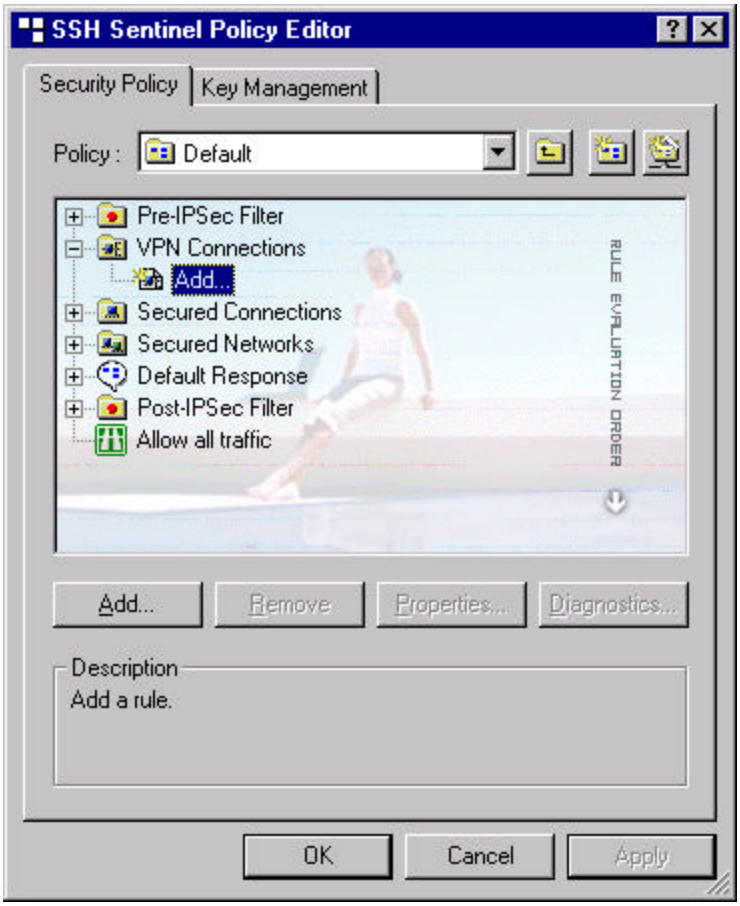
   - Enter a **Name** for the key, a **shared secret** (a secret code), and then **confirm the secret code** by retyping it. The shared secret needs to match what was entered for the RouteFinder.

     Example:
     Key Name = new preshared key
     Shared Secret = 1o2t3t4f

   - Click **Finish.**

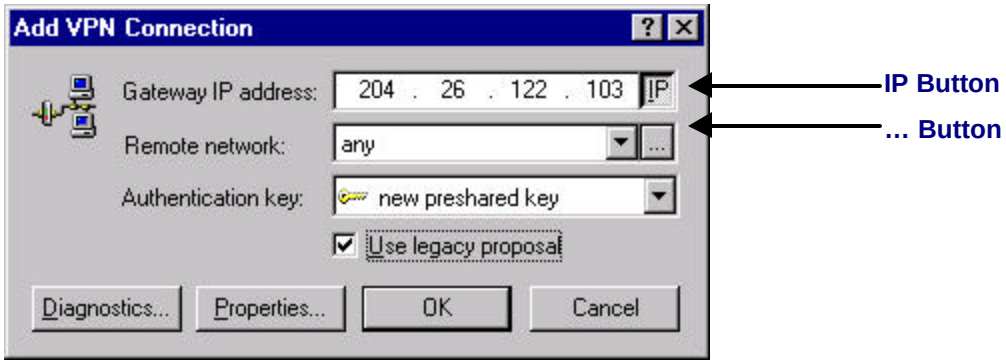
Pre-Shared Key Information
Create Pre-Shared Key
Type in the shared secret.
ssh
Give the pre-shared key a name that is for your reference only. Type the shared secret twice to avoid typos. Use the fingerprint to verify the secret with the other party involved in the communication without revealing the actual secret.
Pre-shared key
Name:
new preshared key
Shared secret:
****
Confirm shared secret:
****
Fingerprint (SHA-1):
f8ba d6d4
< Back
Finish
Cancel

6. This step will start with the **Key Management** tab displayed.
   - First, click the **Apply** button at the bottom of the screen.
   - Then click the **Security Policy** tab.
   - On the **Security Policy** tab, double-click **VPN Connection**
   - Click **Add**.



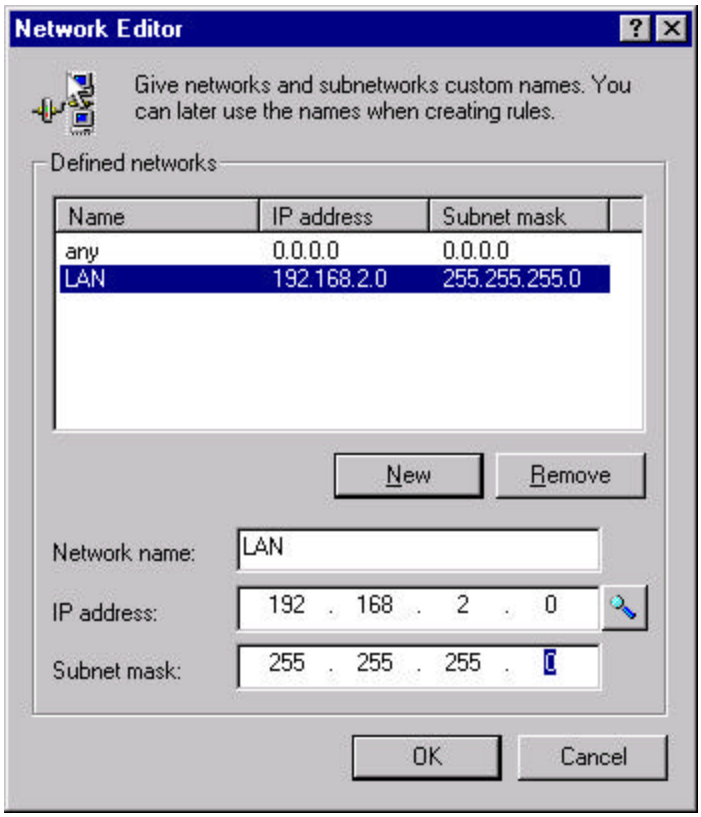
7. On the **Add VPN Connection** screen, enter the Security Gateway information.
   - Click the **IP** button IP at the end of the **Gateway IP Address** field, and enter the public (WAN) **IP Address** of the RouteFinder (Example: 204.26.122.103)
   - Click the down arrow to move to the **Authentication key** field, and select the key name created in the previous step.
   - Check the box for **Use Legacy Proposal**.

- Then click the **...** button at the end of the **Remote Network** field to enter the Remote Network IP address and the Subnet Mask for the LAN side of the RouteFinder (example: 192.168.2.0 and 255.255.255.0).



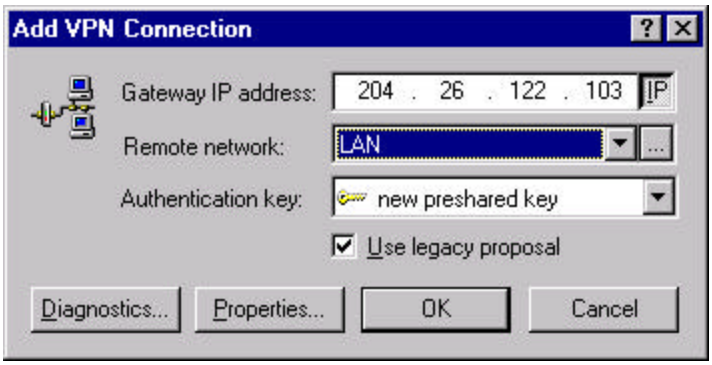
8. After clicking the button in the above dialog box, the **Network Editor** displays.

- Enter the **Remote Network IP** address and the **Subnet mask** for the LAN side of the RouteFinder (example: 192.168.2.0 and 255.255.255.0).
- Click **OK**.



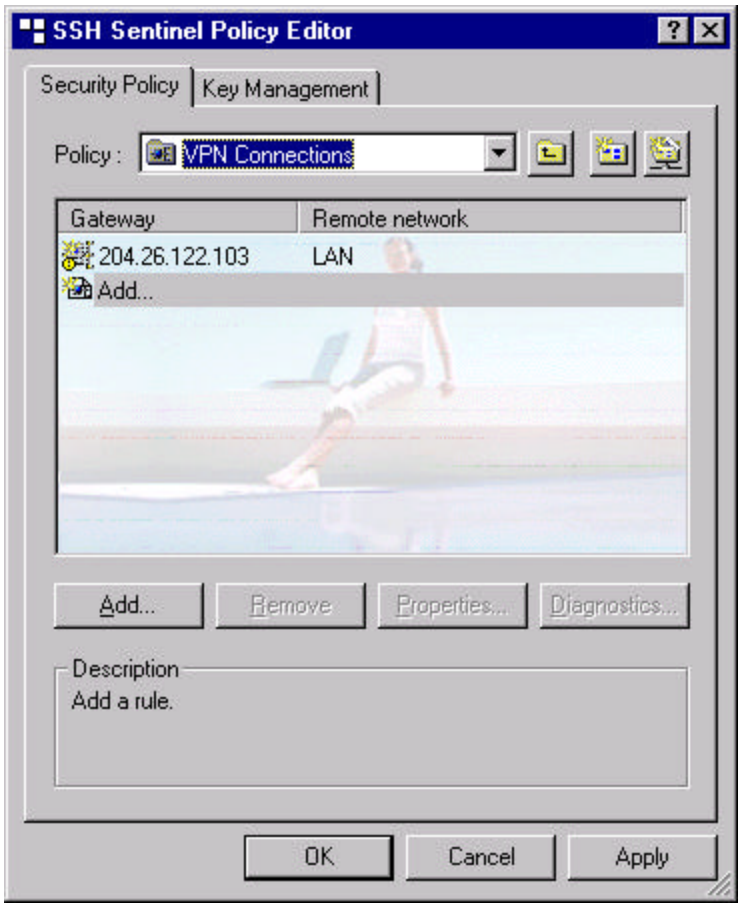
9. Now back at the **Add VPN Connection** screen:

   Click **OK**.

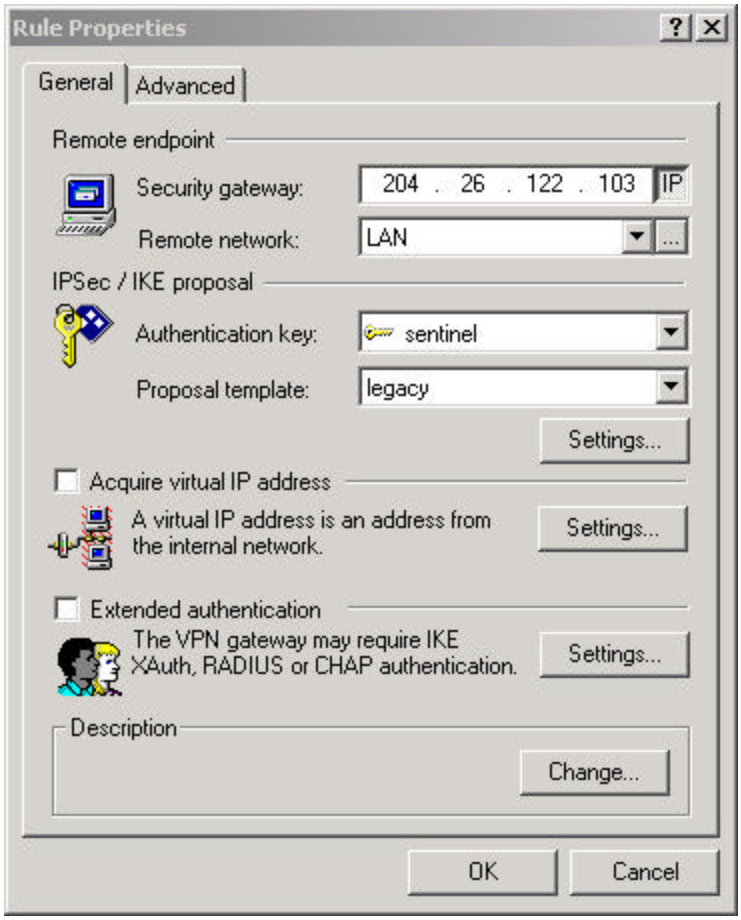


10. Now back at the **Security Policy** tab under the **Policy Editor** screen:

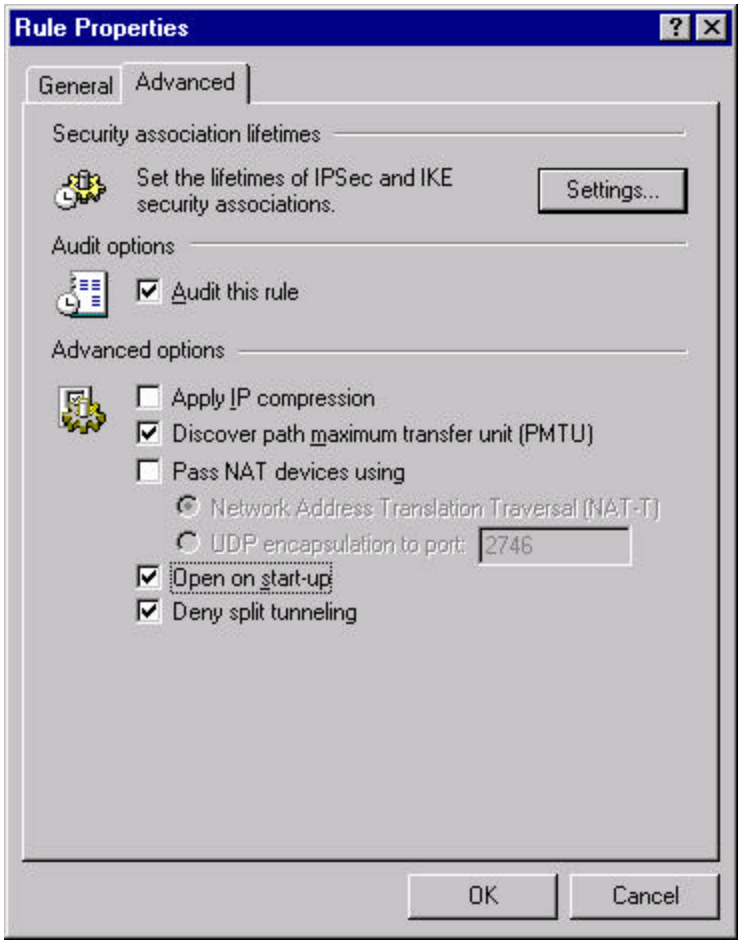
    - Highlight the connection you just created (example: 204.26.122.103).
    - Click the **Properties** button.



11. The **Connection Properties | General** screen displays.
    - Click the **Settings** button under **IPSec / IKE proposal**.
    - Verify that the **PFS Group** is set to **Group 2**.

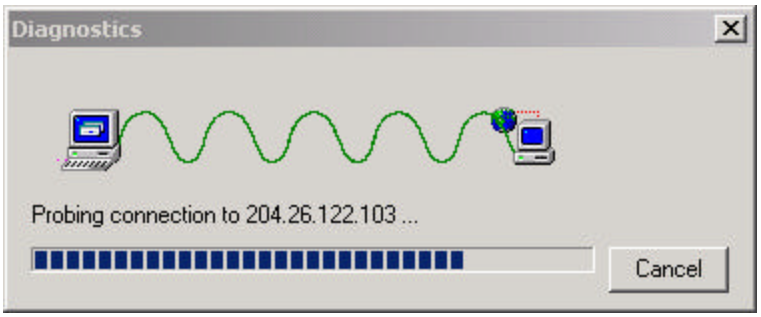


12. Click the **Advanced** tab.
    - Check the box for **Open on start-up**.
    - Click **OK**.
    - Then click **OK** to close the **Rule Properties** screen.



13. Now back at the **Policy Editor** screen:
    - Click the **Apply** button.
    - Double click **VPN Connection**.
    - Highlight the connection you just created (example: 204.26.122.103).
    - Click the **Diagnosis** button.

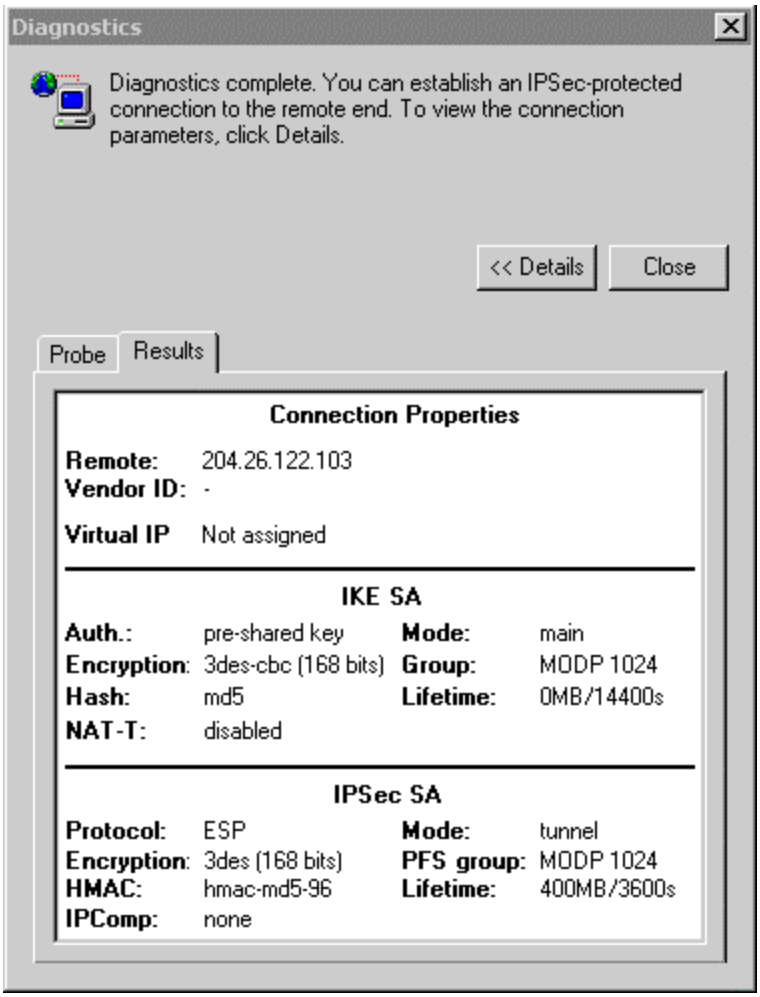
14. Sentinel will probe for a connection to the RouteFinder and should be successful.



15. Click the **Details** button. Details of the newly-created connection display.

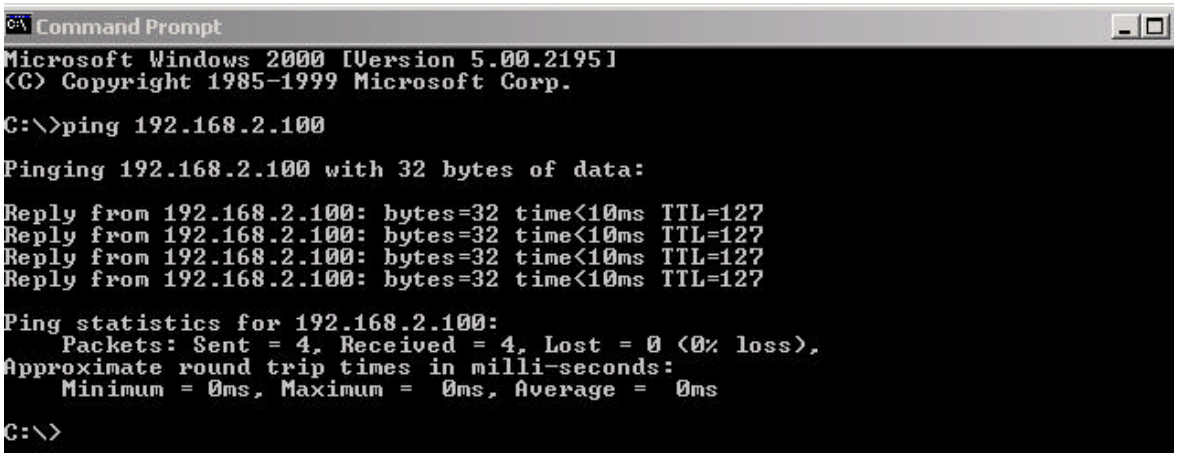
    Verify the connection details information.

    Click **Close**.



16. On the **Policy Editor** screen, click OK to close the **SSH Sentinel** window.

17. Open a DOS command prompt window and attempt to PING the LAN located behind the RouteFinder. If the PING is successful, the configuration process to connect SSH Sentinel client to a RouteFinder is complete. If PING fails, stop and restart the Sentinel Policy Manager. If it still fails, check cabling and software configuration at both locations.



IMPORTANT: The Sentinel Policy Manger may need to be stopped and started in order for you to successfully PING the remote LAN. Once you can PING the remote LAN, do not run the diagnostics test again; otherwise, you will have to stop and start the Policy Manager in order to once again PING successfully.

Chapter 4 – Updating and Removing SSH Sentinel

Updating SSH Sentinel

If you launch the installation package with a previous version of SSH Sentinel software on your computer, the existing version is automatically updated. The contents (i.e., the policies, the rules, the authentication keys, etc.) are preserved. Only the software version is updated.

Removing SSH Sentinel

Before removing the software, you are advised to do the following:
1. Export and save any data in the SSH Sentinel that you might need in the future. For example, you might want to save the trusted root certificates for later use. Since removing the software will delete all files related to the software, save the data in a separate folder.
2. Save all unsaved data in other applications and close all open applications.

To remove the software, use the standard Windows **Remove Programs** procedure:
1. Open **Add/Remove Programs** under **Settings** in the **Start** menu.
2. Select **SSH Sentinel** from the listing.
3. Complete the removal by restarting the computer.

You can re-install the software after completely removing it. Import the saved data to your security policy after installation.

Appendix A – Technical Support

When contacting Multi-Tech, be sure to have your RouteFinder information and details about the functioning of the software.

Contacting Technical Support

Country	Using email	By phone
France	Support@multitech.fr	+(33) 1-64 61 09 81
India	Support@multitechindia.com	+(91) 124-340778
U.K.	Support@multitech.co.uk	+(44) 118 959 7774
Rest of World	Support@multitech.com	800-972-2439 (U.S. & Canada) or +763-785-3500

Recording RouteFinder Information

Before placing a call to our Technical Support staff, record the following information about your Multi-Tech RouteFinder.

Model no.: _____

Serial no.: _____

Firmware version: _____

List information that indicates the status of your RouteFinder in the space provided before calling tech support. Include screen messages, diagnostic test results, problems with a specific application, etc.

_____

_____

Appendix B – SSH Sentinel CD

A CD is provided with your purchase of the SSH Sentinel software. The CD contains the SSH Sentinel software, a complete User Guide, a copy of this Quick Start Guide, and the software license agreement.

When you insert the CD in your computer's CD-ROM drive, the SSH Sentinel software **Install** screen displays.

If the ***Program Not Found*** message displays or if the Auto run feature does not function, click the file ***Autorun.bat*** (

)in the CD's root directory.

Some of the CD selections are described below:

Click **Install IPSEC Client Software** to load the SSH Sentinel software and either run the program from the CD or save it to your computer's hard disk drive.

Click **Read the End User Licensing Agreement** to view the Multi-Tech Multi-User Software License Agreement. Note that the Software License Agreement is also provided in this manual.

Click **Read the Installation User Guide** to view and/or print the full online User Guide manual (published by the SSH Communications Security Corp.) This is an Adobe Acrobat file - if you don't have the Acrobat Reader, download it from http://www.adobe.com.

Click **Read the Installation Quick Start Guide** to view and/or print the online Quick Start Guide (the printed guide included with your purchase). This is an Adobe Acrobat file - if you don't have the Acrobat Reader, download it from http://www.adobe.com.

Appendix C – Multi-User Software License Agreement

Multi-Tech Systems, Inc.
IMPORTANT – READ BEFORE OPENING OR ACCESSING SOFTWARE

This is a basic multi-user software license granted by Multi-Tech Systems, Inc., a Minnesota corporation, with its mailing address at 2205 Woodale Drive, Mounds View, MN 55112.

This is a legal agreement between you (either an individual or a single entity) and Multi-Tech Systems, Inc. for the Multi-Tech software product enclosed, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). The SOFTWARE PRODUCT also includes any updates and supplements to the original SOFTWARE PRODUCT provided to you by Multi-Tech.

Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement.

By installing, copying, downloading, accessing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of that separate end-user license agreement.

This copy of Multi-Tech Systems software is provided only on the condition that you, Customer, agree to the following license agreement. READ THIS LICENSE CAREFULLY. If you do not agree to the terms contained in this license, return the packaged program UNOPENED to the place you obtained it. If you agree to the terms contained in this license, fill out the enclosed Software Registration Card, and return the card by mail. Registration may also be done on Multi-Tech Systems web site at www.multitech.com/register. Opening the packaged program constitutes agreement to be bound by the terms and conditions of this Software License Agreement. Your right to use the software terminates automatically if you violate any part of this software license agreement.

Multi-Tech Software License Agreement
Multi-Tech Systems, Inc. (MTS) agrees to grant and Customer agrees to accept on the following terms and conditions, a non-transferable and non-exclusive license to use the software program(s) delivered with this Agreement.

GRANT OF LICENSE. MTS grants Customer the right to use one copy of the software on a single product (the Licensed System). You may not network the software or otherwise use it on more than one product at the same time.

COPYRIGHT. The software is owned by MTS and is protected by United States copyright laws and international treaty provisions. Therefore, Customer must treat the software like any copyrighted material. Customer may install the software to a single hard disk and keep the original for backup or archival purposes. Customer shall NOT copy, or translate into any language, in whole or in part, any documentation which is provided by MTS in printed form under this Agreement.

OTHER RESTRICTIONS. The software may not be assigned, sublicensed, translated or otherwise transferred by Customer without prior written consent from MTS. Customer may not reverse engineer, decompile, or disassemble the software. Any updates shall be used only on the Licensed System, and shall remain subject to all other terms of this Agreement. Customer agrees not to provide or otherwise make available the software including, but not limited to documentation, programs listings, object code, or source code, in any form, to any person other than Customer and his employees and /or agents, without prior written consent from MTS. Customer acknowledges that the techniques, algorithms, and processes contained in the software are proprietary to MTS and Customer agrees not to use or disclose such information except as necessary to use the software.

Customer shall take reasonable steps consistent with steps taken to protect its own proprietary information to prevent the unauthorized copying or use by third parties of the software or any of the other materials provided under this Agreement. Any previous version of the software must be destroyed or returned to Multi-Tech Systems, Inc. within 90 days of receipt of the software upgrade or update.

LIMITED WARRANTY. MTS warrants that the software will perform substantially in accordance to the product specifications in effect at the time of receipt by Customer. If the MTS software fails to perform accordingly, MTS will optionally repair any defect, or replace it. This warranty is void if the failure has resulted from

accident, abuse, or misapplication. A Software Registration Card must be on file at MTS for this warranty to be in effect. In all other respects, the MTS software is provided AS IS. Likewise, any other software provided with MTS software is provided AS IS.

THE FOREGOING WARRANTY IS IN LIEU ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL MTS BE LIABLE FOR CONSEQUENTIAL DAMAGES RESULTING FROM USE OF THE LICENSED PROGRAM, WHETHER AS A RESULT OF MTS NEGLIGENCE OR NOT, EVEN IF MTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. MTS ALSO DISCLAIMS ANY LIABILITY IN CONTRACT OR OTHERWISE FOR THE DEFECT OR NON-PERFORMANCE OF ANY SEPARATE END-USER LICENSED SOFTWARE PRODUCT INCLUDED WITH MTS' SOFTWARE.

INDEMNIFICATION. MTS will indemnify and defend Customer from any claim that the software infringes on any copyright, trademark, or patent. Customer will indemnify and defend MTS against all other proceedings arising out of Customers use of the software.

GENERAL. If any of the provisions, or portions thereof, of this Agreement are invalid under any applicable statute or rule of law, they are to that extent deemed to be omitted.

This is the complete and exclusive statement of the Agreement between the parties, which supersedes all proposals, oral, written and all other communications between the parties relating to the subject matter of this Agreement. This Agreement may only be amended or modified in writing, signed by authorized representatives of both parties.

This Agreement shall be governed by the laws of the State of Minnesota. The waiver of one breach or default hereunder shall not constitute the waiver of any subsequent breach or default.

Licensee also agrees to the following:
I am not a citizen, national, or resident of, and am not under the control of the government of: Afghanistan, Cuba, Iran, Iraq, Libya, Montenegro, North Korea, Pakistan, Serbia, Sudan, Syria, nor any other country to which the United States has prohibited export. I will not download or by any other means export or re-export the Programs, either directly or indirectly, to the above countries, nor to citizens, nationals or residents of the above countries. I am not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and/or Specially Designated Narcotics Traffickers, nor am I listed on the United States Department of Commerce Table of Denial Orders. I will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists. I will not use the Programs for, and will not allow the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical, or biological weapons of mass destruction.

Licensee agrees that by purchase and/or use of the Software, s/he hereby accepts and agrees to the terms of this License Agreement.

Multi-User Limited Warranty and License Agreement

The software contained in this package is licensed by Multi-Tech Systems, Inc., to the original end-user purchaser, hereafter referred to as Licensee, of this product for site use. A site is defined as a single business, government, or academic location, such as a building, a floor of a building, a campus, etc., and covers no more than 250 users at that location. A licensee may be a Local Area Network administrator, MIS director, purchasing agent, or other representative who acts on behalf of the users at that single site. This license provides for use of the distribution diskette, other accompanying programs, where applicable, and one copy of the documentation.

The software programs and installation utilities, hereafter referred to as Software, consist of the computer program files included on the original distribution diskette(s) or CD-ROM(s).

Licensee agrees that by purchase and/or use of the Software, s/he hereby accepts and agrees to the terms of this License Agreement.

In consideration of mutual covenants contained herein, and other good and valuable considerations, the receipt and sufficiency of which is acknowledged, Multi-Tech Systems, Inc., does hereby grant to the Licensee a non-transferable and non-exclusive license to use the Software and accompanying documentation under the following terms and conditions:

The software is furnished to the Licensee as the single site representative for execution and use on as many workstations as that single site contains, for up to 250 users inclusively. Software and manuals may be copied, with the inclusion of the Multi-Tech Systems, Inc., copyright notice, for use within that single site. Additional manuals may be ordered from Multi-Tech Systems, Inc., for a nominal charge.

This license covers only the stipulated single site. The Licensee hereby agrees not to provide, or otherwise make available, any portion of this software in any form to any third party without the prior express written approval of Multi-Tech Systems, Inc. Licensee is hereby informed that this Software contains confidential, proprietary, and valuable trade secrets developed by or licensed to Multi-Tech Systems, Inc., and agrees that sole ownership shall remain with Multi-Tech Systems, Inc.

The Software and documentation are copyrighted. Except as provided herein, the Software and documentation supplied under this agreement may not be copied, reproduced, published, licensed, sub-licensed, distributed, transferred, or made available in any form, in whole or in part, to others without expressed written permission of Multi-Tech Systems, Inc. Copies of the Software may be made to replace worn or deteriorated copies, for archival, or back-up purposes.

Licensee agrees to implement sufficient security measures to protect Multi-Tech Systems, Inc.'s proprietary interests, and not to allow the use, copying, or transfer by any means, other than in accordance with this agreement.

Licensee agrees that any breach of this agreement will be damaging to Multi-Tech Systems, Inc.

LICENSEE AGREES THAT ALL WARRANTIES, IMPLIED OR OTHERWISE, WITH REGARD TO THIS SOFTWARE, INCLUDING ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR ANY PARTICULAR PURPOSE ARE EXPRESSLY WAIVED, AND NO LIABILITY SHALL EXTEND TO ANY DAMAGES, INCLUDING CONSEQUENTIAL DAMAGES, WHETHER OR NOT KNOWN TO MULTI-TECH SYSTEMS, INC. IT IS HEREBY EXPRESSLY AGREED THAT LICENSEE'S REMEDY IS LIMITED TO REPLACEMENT OR REFUND OF THE LICENSE FEE, AT THE OPTION OF MULTI-TECH SYSTEMS, INC., FOR DEFECTIVE DISTRIBUTION MEDIA. There is no warranty for misused materials.

If this package contains multiple media formats (e.g., both 3.5" disk(s) and CD-ROM), they are provided only to facilitate use at a single site. Neither this Software, nor its accompanying documentation may be modified or translated without the written permission of Multi-Tech Systems, Inc.

This agreement shall be governed by the laws of the State of Minnesota. The terms and conditions of this agreement shall prevail regardless of the terms of any other submitted by the Licensee. This agreement supersedes any proposal or prior agreement. Licensee further agrees that this License Agreement is the complete and exclusive Statement of Agreement, and supersedes oral, written, or any other communications between Multi-Tech Systems, Inc., and Licensee relating to the subject matter of this agreement. This agreement is not assignable without written permission of an authorized agent of Multi-Tech Systems, Inc.

82013152 (C)